Cryptography and Communications
https://doi.org/10.1007/s12095-024-00766-3

RESEARCH

Upper bounds on the numbers of binary plateaued and bent functions

V. N. Potapov[1]

Received: 15 October 2023 / Accepted: 5 December 2024

Abstract
We prove that the logarithm of the number of binary n-variable bent functions is asymptotically less than $\frac{11}{32}2^n$ as $n \to \infty$. We also prove an asymptotic upper bound on the number of s-plateaued functions.

Keywords Boolean function · Walsh–Hadamard transform · Plateaued function · Bent function · Upper bound

Mathematics Subject Classification (2010) 94D10 · 94A60 · 06E30

1 Introduction

Bent functions are maximally nonlinear Boolean functions with an even number of variables and are optimal combinatorial objects. In cryptography, bent functions are used in block ciphers. Moreover, bent functions have many theoretical applications in discrete mathematics. Full classification of bent functions would be useful for combinatorics and cryptography. But constructive classifications and enumerations of bent functions in n variables are likely impossible for large n. The numbers of n-variable bent functions are only known for $n \le 8$. There exist 8 bent functions for $n = 2$, 896 for $n = 4$, approximately $2^{32.3}$ for $n = 6$ and $2^{106.3}$ for $n = 8$ [8]. Thus, lower and upper asymptotic bounds of the number of bent functions are very interesting (see [10, Chapter 4.4], [18, Chapter 13]).

Currently, there exists a drastic gap between the upper and lower bounds on the number of bent functions. Let $\mathcal{N}(n) = \log_2 |\mathcal{B}(n)|$, where $\mathcal{B}(n)$ is the set of Boolean bent functions in n variables. New asymptotic lower bounds on the number of bent functions is recently proven in the binary case [14] and in the case of finite fields of odd characteristic [15]. In the binary case it is $\mathcal{N}(n) \ge \frac{3n}{4}2^{n/2}(1 + o(1))$ as n is even and $n \to \infty$. This bound is slightly better than the bound $\mathcal{N}(n) \ge \frac{n}{2}2^{n/2}(1 + o(1))$ based on the Maiorana–McFarland construction of bent functions. It is well known (see e.g. [2, 4, 10]) that the algebraic degree of a binary bent function in n variables is not greater than $n/2$. Therefore, $\mathcal{N}(n) \le \sum_{i=0}^{n/2} \binom{n}{i} = 2^{n-1} + \frac{1}{2}\binom{n}{n/2}$. There are some nontrivial upper bounds of $|\mathcal{B}(n)|$. But, bounds from [3] and [1] are of the

✉ V. N. Potapov
vpotapov@math.nsc.ru

[1] Sobolev Institute of Mathematics, Novosibirsk, Russia

same type $\mathcal{N}(n) \leq 2^{n-1}(1 + o(1))$ up to the asymptotic of logarithm. An upper bound $\mathcal{N}(n) \leq \frac{3}{4} \cdot 2^{n-1}(1 + o(1))$ is proven in [12]. In this paper we improved latter bound and obtained that $\mathcal{N}(n) < \frac{11}{16} \cdot 2^{n-1}(1 + o(1))$ (Theorem 2). Note that Tokareva's conjecture (see [17] and [10]) on the decomposition of Boolean functions into sums of bent functions implies that $\mathcal{N}(n) \geq \frac{1}{2}2^{n-1} + \frac{1}{4}\binom{n}{n/2}$.

The new bound mentioned above is asymptotic. One can use the proposed method to find a non-asymptotic upper bound on the number of bent functions. But for the fixed $n = 6$ and $n = 8$ such bound is greater than $\frac{11}{32} \cdot 2^n$ approximately twice. The main reason of this difference lies in the cardinality of the middle layer of the n-dimensional Boolean cube. This cardinality is asymptotically negligible, but that is not in the case for $n = 6$ and $n = 8$.

The new upper bound on the number of bent functions is based on new asymptotic upper bound on the number of s-plateaued Boolean functions in n variables. s-Plateaued functions are a generalization of bent functions which are the same as 0-plateaued functions. Plateaued functions can combine important cryptographic properties of nonlinearity and correlation immunity (see e.g. [6]). Let $\mathcal{N}(n, s)$ be the logarithm of the number of such functions. In Theorem 1 (a) we prove that

$$\mathcal{N}(n,s) \leq \left(b\left(n-2, \left\lceil \frac{n-s}{2} \right\rceil + 1\right)\left(1 + \frac{3}{8}\log 6\right) + 2^{n-2}\left(\hbar\left(\frac{1}{2^s}\right) + \frac{1}{2^s}\right)\right)(1+o(1))$$

as $n \to \infty$, where $\hbar$ is Shannon's entropy function and $b(n, r)$ is the cardinality of balls with radius r in the n-dimensional Boolean cube. This bound is not tight but sufficient to disprove the following conjecture on derivatives of bent functions. Tokareva (see [19, 21]) conjectured that each balanced Boolean function f in an even number of variables n of algebraic degree at most $n/2 - 1$ is a derivative of some bent function if $f(x) = f(x \oplus y)$ for every vector x and some nonzero vector y. It is true for $n \leq 6$ [21, Theorem 4] but based on Theorem 1 (b) it is proved that this conjecture is false when n is large enough (see [16]).

The method of proving the above bounds implies a storage algorithm for bent and plateaued functions. Essentially we calculate the number of bits needed to define all the values of the function. A quantity of bits required by the algorithm is equal to the corresponding upper bound $\mathcal{N}(n, s)$. In practice we need bent and plateaued functions with some special properties. See, for example, some recent constructions from [5, 9] and [22]. Therefore, methods of compact storage of n-variable bent and plateaued functions may be useful for large n.

2 Fourier transform

Let $\mathbb{F} = \{0, 1\}$. The set $\mathbb{F}^n$ is called a Boolean hypercube (or a Boolean n-cube). $\mathbb{F}^n$ equipped with coordinate-wise modulo 2 addition $\oplus$ can be considered as an n-dimensional vector space. Functions $\phi_x(y) = (-1)^{\langle x,y\rangle}$ are called characters. Here $\langle x, y\rangle = x_1y_1 \oplus \cdots \oplus x_ny_n$ is the inner product. Let G be a function that maps from the Boolean hypercube to real numbers. The Fourier transform of G is defined by the formula $\widehat{G}(y) = (G, \phi_y) = \sum_{x\in\mathbb{F}^n} G(x)(-1)^{\langle x,y\rangle}$, i.e., $\widehat{G}(y)$ are the coefficients of the expansion of G with respect to the basis of characters. We can define the Walsh–Hadamard transform of a Boolean function $f : \mathbb{F}^n \to \mathbb{F}$ by the formula $W_f(y) = \widehat{(-1)^f}(y)$, i.e.,

$$W_f(y) = \sum_{x\in\mathbb{F}^n} (-1)^{f(x)\oplus\langle x,y\rangle}.$$

A Boolean function b is called a bent function if $W_b(y) = \pm 2^{n/2}$ for all $y \in \mathbb{F}^n$. So, $W_b = 2^{n/2}(-1)^g$ for some Boolean function g. It is well known (see e.g. [2, 10]) that g is also a bent function and $W_g = 2^{n/2}(-1)^b$. Such bent functions b and g are called dual. It is easy to see that n-variable bent functions exist only if n is even. A Boolean function p is called an s-plateaued function if $W_p(y) = \pm 2^{(n+s)/2}$ or $W_p(y) = 0$ for all $y \in \mathbb{F}^n$. So, bent functions are 0-plateaued functions. 1-Plateaued functions are called near-bent.

From Parseval's identity

$$\sum_{y\in\mathbb{F}^n} \widehat{H}^2(y) = 2^n \sum_{x\in\mathbb{F}^n} H^2(x),$$

where $H : \mathbb{F}^n \to \mathbb{R}$, it follows straightforwardly:

Proposition 1 *For every s-plateaued function, a part of nonzero values of its Walsh–Hadamard transform is equal to $\frac{1}{2^s}$.*

It is well known (see e.g. [2],[20]) that for any function $H, G : \mathbb{F}^n \to \mathbb{R}$ it holds

$$\widehat{H * G} = \widehat{H} \cdot \widehat{G} \quad \text{and} \quad \widehat{(\widehat{H})} = 2^n H,$$

where $H * G(z) = \sum_{x\in\mathbb{F}^n} H(x)G(z \oplus x)$ is a convolution. Consequently, it holds

$$2^n H * G = \widehat{\widehat{H} \cdot \widehat{G}} \text{ and } \widehat{H} * \widehat{G} = 2^n \widehat{H \cdot G}. \tag{1}$$

Let Γ be a subspace of the hypercube.

Denote by $\Gamma^\perp$ a dual subspace, i.e., $\Gamma^\perp = \{y \in \mathbb{F}^n : \forall x \in \Gamma, \langle x, y\rangle = 0\}$. Let $\mathbf{1}_S$ be an indicator function for $S \subset \mathbb{F}^n$. It is easy to see that for every subspace Γ it holds $\widehat{\mathbf{1}_{\Gamma^\perp}} = 2^{n-\dim\Gamma}\mathbf{1}_\Gamma$. By (1) we have

$$H * \mathbf{1}_{\Gamma^\perp} = 2^{-\dim\Gamma}\widehat{\widehat{H} \cdot \mathbf{1}_\Gamma} \tag{2}$$

for any subspace $\Gamma \subset \mathbb{F}^n$. When we substitute vector $a \in \mathbb{F}^n$ in (2) we obtain

$$\sum_{x\in a\oplus\Gamma^\perp} H(x) = 2^{-\dim\Gamma}\sum_{y\in\Gamma} \widehat{H}(y)(-1)^{y\oplus a}. \tag{3}$$

Denote by $\mathrm{supp}(G) = \{x \in \mathbb{F}^n : G(x) \neq 0\}$ the support of G. Without any confusion, we will consider the support of a real-valued function as a Boolean function. We need the following known property of bent functions (see e.g. [10]).

Proposition 2 *Let f be an n-variable bent function and let Γ be a hyperplane obtained by fixing one coordinate to 0. Consider $h = f \cdot \mathbf{1}_\Gamma$ as an $(n-1)$-variable function. Then h is a 1-plateaued function.*

Proof By the definition we have $2^{n/2}(-1)^f = \widehat{(-1)^g}$, where a bent function g is dual of f. By (2)

$$2^{\frac{n}{2}-1}(-1)^g * \mathbf{1}_{\Gamma^\perp} = \widehat{(-1)^f \cdot \mathbf{1}_\Gamma}.$$

For a nonzero $a \in \Gamma^\perp$ and any $x \in \Gamma$ we obtain

$$(-1)^g * \mathbf{1}_{\Gamma^\perp}(x) = (-1)^g(x) + (-1)^g(x \oplus a) = \pm 2 \text{ or } 0.$$

Then $\widehat{(-1)^f \cdot \mathbf{1}_\Gamma}(x) = \pm 2^{\frac{(n-1)+1}{2}}$ or 0. It is easy to see that $\widehat{(-1)^h}(x) = \widehat{(-1)^f \cdot \mathbf{1}_\Gamma}(x) = \widehat{(-1)^f \cdot \mathbf{1}_\Gamma}(x \oplus a)$. Consequently, h is a 1-plateaued function by the definition. □

Proposition 3 *Suppose that f and g are Boolean functions in n variables. For any subspace $\Gamma \subset \mathbb{F}^n$ if $W_f|_\Gamma = W_g|_\Gamma$ then $\sum_{x \in z \oplus \Gamma^\perp} (-1)^{f(x)} = \sum_{x \in z \oplus \Gamma^\perp} (-1)^{g(x)}$ for any $z \in \mathbb{F}^n$.*

Proof It follows from (2). Indeed it holds $\widehat{(-1)^f} \cdot \mathbf{1}_\Gamma = \widehat{(-1)^g} \cdot \mathbf{1}_\Gamma$ by the conditions of the lemma. Then $(-1)^f * \mathbf{1}_{\Gamma^\perp} = (-1)^g * \mathbf{1}_{\Gamma^\perp}$. It is clear that $((-1)^f * \mathbf{1}_{\Gamma^\perp})(z) = \sum_{x \in z \oplus \Gamma^\perp} (-1)^{f(x)}$. This completes the proof. □

3 Möbius transform

Denote by $\mathrm{wt}(z)$ the number of units in $z \in \mathbb{F}^n$. Every Boolean function f can be represented in the algebraic normal form:

$$f(x_1, \ldots, x_n) = \bigoplus_{y \in \mathbb{F}^n} M[f](y) x_1^{y_1} \cdots x_n^{y_n}, \tag{4}$$

where $x^0 = 1, x^1 = x$, and $M[f] : \mathbb{F}^n \to \mathbb{F}$ is the Möbius transform of f. It is well known that

$$M[f](y) = \bigoplus_{x \in \Gamma_y} f(x) \tag{5}$$

where $\Gamma_y = \{(x_1, \ldots, x_n) \in \mathbb{F}^n : x_i = 0 \text{ if } y_i = 0\}$ is a subspace of $\mathbb{F}^n$. Note that $M[M[f]] = f$ for each Boolean function (see [2, Theorem 1]). The degree of this polynomial is called the algebraic degree of f.

Denote by $b(n, r)$ the cardinality of a ball $B_{n,r}$ with radius r in $\mathbb{F}^n$, i.e., $b(n, r) = |\{x \in \mathbb{F}^n : \mathrm{wt}(x) \le r\}|$. By properties of the Möbius transform, the number of n-variable Boolean functions f such that $\deg f \le r$ is equal to $2^{b(n,r)}$.

Lemma 1 *Suppose that f and g are n-variable Boolean functions and $\max\{\deg(f), \deg(g)\} \le r$. If $f|_{B_{n,r}} = g|_{B_{n,r}}$ then $f = g$.*

Proof By the hypothesis of the lemma and (4), we have $M[f](y) = M[g](y) = 0$ if $\mathrm{wt}(y) > r$. By (5) for any $y \in \mathbb{F}^n$ such that $\mathrm{wt}(y) = r + 1$, we obtain

$$M[f](y) = \bigoplus_{x \in \Gamma_y} f(x) = f(y) \oplus \bigoplus_{x \in \Gamma_y \cap B_{n,r}} f(x)$$

$$= f(y) \oplus \bigoplus_{x \in \Gamma_y \cap B_{n,r}} g(x) = f(y) \oplus M[g](y) \oplus g(y).$$

Therefore, $f(y) = g(y)$ for any $y \in B_{n,r+1}$. By induction on weights $\mathrm{wt}(y)$, we obtain that $f(y) = g(y)$ for all $y \in \mathbb{F}^n$. □

Lemma 2 ([2], Theorem 2) *Let f be an n-variable Boolean function. Suppose for every $y \in \mathbb{F}^n$ it holds $\widehat{(-1)^f}(y) = 2^k m(y)$, where $m(y)$ is integer. Then $\deg(f) \le n - k + 1$.*

Corollary 1 ([2], Proposition 96) *The algebraic degree of n-variable s-plateaued functions is not greater than $\frac{n-s}{2} + 1$.*

Note that algebraic degrees of bent (0-plateaued) functions is $n/2$ at most (see e.g. [2], [4], [10]), but for 1-plateaued functions the upper bound $\frac{n+1}{2}$ is sharp.

Proposition 4 *Let f be an n-variable bent function. Then for any hyperplane Γ the algebraic degree of the Boolean function $h = \mathrm{supp}(\widehat{(-1)^f} \cdot \mathbf{1}_\Gamma)$ is not greater than $n/2$.*

Proof By (2) we obtain that $h = \mathrm{supp}((-1)^g * \mathbf{1}_{\Gamma^\perp})$, where a bent function g is dual of f. Let $\Gamma^\perp = \{\bar{0}, a\}$. Then $(-1)^g * \mathbf{1}_{\Gamma^\perp}(x) = (-1)^{g(x)} + (-1)^{g(x\oplus a)}$. Consequently, $h(x) = g(x) \oplus g(x \oplus a) \oplus 1$. Thus, $\deg h \le \deg g \le \frac{n}{2}$. □

4 Subspace distribution

We will use the following well-known criterium (see, e.g. [2, Proposition 96]) which is also true in the nonbinary case ([11, Theorem 2]).

Lemma 3 *An n-variable Boolean function f is s-plateaued if and only if it holds $(-1)^f * (-1)^f * (-1)^f = 2^{n+s}(-1)^f$.*

Consider an n-variable s-plateaued Boolean function f and any fixed $x \in \mathbb{F}^n$. There are $V = \begin{bmatrix} n \\ 2 \end{bmatrix}_2 = \frac{(2^n-1)(2^n-2)}{6}$ 2-dimensional affine subspaces such that any of them contains x. Let $S(x)$ be the number of subspaces containing an odd number of zero values of f. By Lemma 3 we obtain

Proposition 5 *For any fixed $x \in \mathbb{F}^n$, it holds $\frac{S(x)}{V} = \frac{1}{2} - \frac{1}{2} \cdot \frac{2^{n+s}-3\cdot 2^n+2}{(2^n-1)(2^n-2)}$.*

Proof We can rewrite the formula from Lemma 3 by the following form

$$2^{n+s}(-1)^{f(x)} = \sum_{z\in\mathbb{F}^n} \sum_{y\in\mathbb{F}^n} (-1)^{f(y)\oplus f(y\oplus z)\oplus f(x\oplus z)} = \sum_{z\in\mathbb{F}^n} \sum_{y\in\mathbb{F}^n} (-1)^{f(x\oplus y)\oplus f(x\oplus y\oplus z)\oplus f(x\oplus z)}.$$

It is easy to see that if two elements of $\{x, x\oplus y, x\oplus z, x\oplus y\oplus z\}$ are coincide then the two remaining elements are also coincide. In this case $(-1)^{f(x)\oplus f(x\oplus y)\oplus f(x\oplus z)\oplus f(x\oplus y\oplus z)} = 1$. Let U be the set of such couples $\{y, z\}$ that $\{x, x \oplus y, x \oplus z, x \oplus y \oplus z\}$ is a 2-dimensional affine subspace. By the inclusion-exclusion formula, we obtain that

$$\sum_{\{y,z\}\in U} (-1)^{f(x)\oplus f(x\oplus y)\oplus f(x\oplus z)\oplus f(x\oplus y\oplus z)} = 2^{n+s} - 3\cdot 2^n + 2.$$

It is easy to see that every subspace $\{x, x \oplus y, x \oplus z, x \oplus y \oplus z\}$ occurs 6 times in the sum above. Consequently, it holds equation

$$\frac{2^{n+s} - 3\cdot 2^n + 2}{6} = (V - S(x)) - S(x).$$

The extraction of $\frac{S(x)}{V}$ from the last equation completes the proof. □

Thus we have two equations: $\frac{S(x)}{V} = \frac{1}{2} + \frac{1}{2(2^{n-1}-1)}$ for every bent function and $\frac{S(x)}{V} = \frac{1}{2} + \frac{1}{2(2^n-1)}$ for every 1-plateaued function. Note that for bent functions f, $f(\bar{0}) = 0$, numbers of linear subspaces such that contain 1, 2, 3 or 4 zero values of f do not depend on f (see [13]).

We will use the following property of bent and plateaued functions.

Proposition 6 *([2, 4, 10]) Let $f : \mathbb{F}^n \to \mathbb{F}$ be an s-plateaued function, let $A : \mathbb{F}^n \to \mathbb{F}^n$ be a non-degenerate affine transformation and let $\ell : \mathbb{F}^n \to \mathbb{F}$ be an affine function. Then $g = (f \circ A) \oplus \ell$ is an s-plateaued function.*

The functions f and g satisfied the conditions of Proposition 6 are called EA-equivalent. It is easy to see that the cardinality of any equivalence class is not greater than $a_n = 2^{n^2+n+1}(1 + o(1))$. Note that two EA-equivalent functions f and g have the same algebraic degree as $\deg(f) > 1$.

There are eight 2-variable Boolean functions such that take value 0 even times. All of them are affine. Six of them take value 0 two times and the other take value 0 four or zero times. Consider a 2-dimensional affine subspace Γ and an n-variable Boolean function g. Let g take value 0 even times on Γ. It is easy to see that 3/4 among functions of the set $\{g \oplus \ell : \ell \text{ is an affine function}\}$ take value 0 two times and the other take value 0 four or zero times. Consequently, from Propositions 5 and 6 we deduced:

Corollary 2 *Let Γ be a 2-dimensional face, i.e, axes-aligned plane which can be obtained by fixed all with the exception of two coordinates, and let $f : \mathbb{F}^n \to \mathbb{F}$ be an s-plateaued function. There exists a non-degenerate affine transformation A and an affine function ℓ such that the s-plateaued function $g = (f \circ A) \oplus \ell$ satisfies the following conditions.*

(a) *The part of faces $\Gamma \oplus y$, $y \in \mathbb{F}^n$, that contain an odd number of zero values of g, is less than $\frac{1}{2}$ if $s > 1$ and less than $\frac{1}{2} + \frac{1}{2^n}$ if $s = 1$.*
(b) *Among the faces $\Gamma \oplus y$, $y \in B_{n,r} \subset \mathbb{F}^n$, that contain an even number of zero values of g, not less than one fourth part contain four or zero values* 0.

Proof Firstly, we can find A to provide condition (a). Let $s > 1$. Suppose that the fraction of faces $A^{-1}(\Gamma \oplus y)$, $y \in \mathbb{F}^n$, containing an odd number of zero values of f, is not less than $\frac{1}{2}$ for every non-degenerate affine transformation A. Then at least half of 2-dimensional affine subspaces contain odd numbers of zero values of f. It is contradict to Proposition 5. Therefore, we can fixed a non-degenerate affine transformation A such that $g = f \circ A$ satisfies condition (a). The case $s = 1$ is similar.

Secondly, we can find ℓ to satisfy condition (b). Indeed, we can choose ℓ to provide (b), since as mentioned above, this distribution is on the average for all ℓ. By adding any affine function we save the parity of the number of zero values of g on every 2-dimensional affine subspace. So, we preserve condition (a). Consider the distribution of even numbers of zero values of g on the faces $\Gamma \oplus y$, $y \in \mathbb{F}^n$. It is easy to see that the average distribution over balls with fixed radius r and centers $y \in \mathbb{F}^n$ is equal to the distribution over the Boolean hypercube. Then there exists a ball with center $e \in \mathbb{F}^n$ such that $g = (f \circ A) \oplus \ell$ has the same or better distribution on the ball with center e. Then we can exchange A to $A \oplus e$ to provide the required distribution on $B_{n,r}$. □

Note that a random Boolean function has the required distribution of zero values in a 2-dimensional face, i.e., zero or four 0s with probability $\frac{1}{8}$, one or three 0s with probability $\frac{1}{2}$, two 0s with probability $\frac{3}{8}$.

Let p_0 be a probability of an even number of zero values in a 2-dimensional face and let p_1 be a probability of an odd number of zero values in a 2-dimensional face. Moreover, p'_0 is the probability of two zero values in a 2-dimensional face and $p'_0 \le 3p_0/4$. How many bits on average we need to count four values $(-1)^{g(x)}$ in a 2-dimensional face $\Gamma \oplus y$ from their sum? We use the following simple proposition.

Proposition 7 *Let M be a set of words with length n and let $k_i > 0$ be a number of different symbols in ith place in every word from M. If $p_m = |\{i \in \{1, \ldots, n\} : k_i = m\}|/n$ then*

$$\frac{\log_2 |M|}{n} = \sum_m p_m \log_2 m.$$

Proof By the definition, $|M| = \prod_{i=1}^{n} k_i$. Rearranging the factors, we obtain that $|M| = \prod_m m^{p_m n}$. Taking the logarithm of both sides of the previous equality we deduce the required equality. □

Consequently, to find all values of function in a 2-dimensional face in the case of two zero values we need $\log_2 6$ bits, in the case of odd zero value we need 2 bits, in the case of 0 or 4 zero values we do not need extra bits. Therefore, under conditions (a) and (b) from Corollary 2, it is sufficient $p_0' \log_2 6 + 2p_1 \le 1 + \frac{3}{8}\log_2 6 = \alpha \approx 1.969$ (or $1 + \frac{1}{2^{n-1}} + \frac{3}{8}\log_2 6 = \alpha_n$ if $s = 1$) bits on average for finding four values $(-1)^{g(x)}$ in a 2-dimensional face $\Gamma \oplus y$ from their sum. It is easy to see that $\alpha_n \to \alpha$ as $n \to \infty$. So, we obtain the following statement from Corollary 2 and Proposition 7.

Corollary 3 *For every n-variable s-plateaued function there exists an EA-equivalent function g and 2-dimensional face Γ such that if we know sums of values of $(-1)^g$ on all $\Gamma \oplus y$, $y \in B_{n,r}$, then it is sufficient $\alpha b(n, r)$ (or $\alpha_n b(n, r)$ if $s = 1$) extra bits to identify g on $B_{n,r}$.*

5 Main results

In the previous section we proved that in every EA-equivalence class there exists an s-plateaued function f satisfying the conditions of Corollary 2. Now we estimate the number of bits sufficient to determine f. We will use the following combinatorial version of Shannon's source coding theorem.

Proposition 8 *(see e.g. [7]) Let M_n be a set of equally composed words with length n over alphabet $\mathcal{A}$ and let $p_i > 0$ be a frequency of ith symbol of $\mathcal{A}$ in every word from M_n. Here $\sum_{i=1}^{|\mathcal{A}|} p_i = 1$. Then*

$$\frac{\log_2 |M_n|}{n} = \sum_{i=1}^{|\mathcal{A}|} p_i \log_2 \frac{1}{p_i} + \varepsilon(n, M_n),$$

where $\sup_{M_n} |\varepsilon(n, M_n)| \to 0$ as $n \to \infty$.

The sum $\sum_i p_i \log_2 \frac{1}{p_i}$ is called Shannon's entropy of source with probability p_i of ith symbol. Denote by $\hbar$ Shannon's entropy function in the case of two symbols, i.e., $\hbar(p) = -p \log p - (1-p)\log(1-p)$ for $p \in (0, 1)$.

Let $\mathcal{N}(n, s)$ be the binary logarithm of the number of n-variable s-plateaued Boolean functions. The logarithm of the number of bent functions we denoted by $\mathcal{N}(n)$. Since the Walsh–Hadamard transform is a bijection, $\mathcal{N}(n, s)$ is not greater than the number of bits such that is sufficient to identify W_f for an s-plateaued function f. Therefore, by Shannon's source coding theorem and Proposition 1 we obtain inequality:

$$\mathcal{N}(n, s) \le 2^n \left(\hbar\left(\frac{1}{2^s}\right)(1 + o(1)) + \frac{1}{2^s} \right). \tag{6}$$

Let $\mathcal{N}_0(n, 1)$ be the binary logarithm of the number of n-variable 1-plateaued Boolean functions which are obtained by the restriction of domain of $(n+1)$-variable bent functions to hyperplanes.

Theorem 1 (a) $\mathcal{N}(n, s) \le (\alpha b(n - 2, \lceil \frac{n-s}{2} \rceil + 1) + 2^{n-2}(\hbar(\frac{1}{2^s}) + \frac{1}{2^s}))(1 + o(1))$ *where $\alpha = 1 + \frac{3}{8}\log_2 6$, $s > 0$ is fixed and $n \to \infty$.*

(b) $\mathcal{N}_0(n,1) \le b(n-2,\frac{n+1}{2})(\alpha+\frac{3}{2})(1+o(1))$ *as* $n \to \infty$.

Proof Let f be an n-variable s-plateaued function. Consider an $(n-2)$-dimensional face Γ. Without loss of generality (see Propositions 1 and 6) we admit that the part of nonzero values of W_f in Γ is not greater than $\frac{1}{2^s}$.

Case (a). For every s-plateaued Boolean function f it is sufficient (by similar way as in (6)) $2^{n-2}(\hbar(\frac{1}{2^s})+\frac{1}{2^s})(1+o(1))$ bits to identify $W_f \cdot \mathbf{1}_\Gamma$.

Case (b). Suppose that a 1-plateaued function f is obtained by the restriction of domain of a bent function to a hyperplane. By Proposition 4, an algebraic degree of the support S of the Walsh–Hadamard transform of such 1-plateaued function is not greater than $\frac{n+1}{2}$. By Lemma 1, it is sufficient to identify S only in a ball $B_{n-2,\frac{n+1}{2}}$. Then we just need $(\hbar(\frac{1}{2})+\frac{1}{2})b(n-2,\frac{n+1}{2})(1+o(1)) = \frac{3}{2}b(n-2,\frac{n+1}{2})(1+o(1))$ bits to identify $W_f \cdot \mathbf{1}_\Gamma$ by (6).

The last part of the proof is the same for cases (a) and (b).

By (3), if we know $W_f \cdot \mathbf{1}_\Gamma$ then we can find sums $\sum_{x \in \Gamma^\perp \oplus a} (-1)^{f(x)}$ for any $a \in \mathbb{F}^n$. By Corollary 2, we can choose an s-plateaued function such that is EA-equivalent to f and has the appropriate distribution of these sums. By Corollary 1, an algebraic degree of any n-variable s-plateaued Boolean functions f is not greater than $r = \lceil \frac{n-s}{2} \rceil + 1$. Consequently, by Lemma 2 it is sufficient to recognize values of f in a ball of radius r. By Corollary 3, there exists s-plateaued function f' from the same EA–equivalence class as f such that $\alpha b(n,r)$ if $s > 1$ or $\alpha_n b(n,r)$ if $s = 1$ bits is sufficient to recover f' on $\mathbb{F}^n$. If we know a EA–equivalence class of the function then it is sufficient $\log_2 a_n = n^2+n+1 = o(2^n)$ bits to identify the function. Thus, if $W_f \cdot \mathbf{1}_\Gamma$ is given then we need $\alpha b(n-2, \lceil \frac{n-s}{2} \rceil + 1)(1+o(1))$ extra bits to identify $(-1)^f$. □

Corollary 4 $\mathcal{N}_0(n,1) < 3.47 \cdot 2^{n-3}(1+o(1))$ *as* $n \to \infty$.

The idea of the new upper bound on the number of the Boolean bent functions is the following. We consider a restriction of the domain of a bent function into a hyperplane. This is a 1-plateaued function and we can evaluate the number of such functions by Theorem 1 (b). Then we evaluate the number of extra bits witch we need to recover all values the bent function when we know it values only on hyperplane. By Lemma 1 it is sufficient to identify an n-variable bent function only on a ball with radius $n/2$.

Theorem 2 $\mathcal{N}(n) \le \mathcal{N}_0(n-1,1) + 2^{n-3}(1+o(1)) < \frac{11}{32}2^n(1+o(1))$ *as* $n \to \infty$.

Proof Let f be an n-variable bent function and let g be dual of f bent function. By Proposition 2, $g \cdot \mathbf{1}_\Gamma$ is an $(n-1)$-variable 1-plateaued function as Γ is a hyperplane. Presume that $\Gamma^\perp = \{\bar{0}, a\}$.

Now we evaluate a number of extra bits which is sufficient to recover f if $g \cdot \mathbf{1}_\Gamma$ is given. By (3) we obtain that sums $s(x) = (-1)^{f(x)} + (-1)^{f(x+a)}$ are determined by $g \cdot \mathbf{1}_\Gamma$. Since all derivatives of each bent function are balanced (see e.g. [2], Theorem 12), a half of these sums $s(x)$ are equal to ± 2 and the other half of these sums are equal to 0. In the first case we can extract $(-1)^{f(x)}$ and $(-1)^{f(x+a)}$ from the sum. But in the second case we need an additional information to choose $(-1)^{f(x)} = 1$ and $(-1)^{f(x+a)} = -1$ or vice versa. Denote by S_1 the set of $x \in \Gamma$ such that $s(x) = \pm 2$.

By Lemma 1 and Proposition 6, we need to identify values of f only in some ball with radius $n/2$. It is easy to see that we can find a ball B such that $|S_1 \cap B \cap \Gamma| \ge |B \cap \Gamma|/2$. Therefore, it is necessary not greater than $|B \cap \Gamma| - |S_1 \cap B \cap \Gamma| \le |B \cap \Gamma|/2 = 2^{n-3}(1+o(1))$ extra bits to recover f from $g \cdot \mathbf{1}_\Gamma$. Therefore, we establish that

$$\mathcal{N}(n) \le \mathcal{N}_0(n-1,1) + 2^{n-3}(1+o(1))$$

as $n \to \infty$. By Theorem 1(b), we obtain the required inequality. □

Acknowledgements The author is grateful to S. Avgustinovich and S. Agievich for their attention to this work and useful discussions.

Author Contributions V. Potapov wrote the manuscript text at all.

Funding The research has been carried out within the framework of a state assignment of the Ministry of Education and Science of the Russian Federation for the Institute of Mathematics of the Siberian Branch of the Russian Academy of Sciences (project no. FWNF-2022-0017).

Declarations

Competing interests The authors declare no competing interests.

References

1. Agievich, S.V.: On the continuation to bent functions and upper bounds on their number. Prikl. Diskr. Mat. Suppl. **13**, 18–21 (2020) (in Russian)
2. Carlet, C.: Boolean Functions for Cryptography and Coding Theory. pp. 562. Cambridge University Press, (2020)
3. Carlet, C., Klapper, A.: Upper bounds on the number of resilient functions and of bent functions. In: Proc. of the 23rd Symposium on Information Theory in the Benelux. Louvain-La-Neuve, Belgium (2002)
4. Carlet, C., Mesnager, S.: Four decades of research on bent functions. Des. Codes Cryptogr. **78**(1), 5–50 (2016)
5. Jeong, J., Lee, Y.: Algorithms for constructing balanced plateaued functions with maximal algebraic degrees. IEEE Trans. Inf. Theory **70**(2), 1408–1421 (2024)
6. Khalyavin, A.V., Lobanov, M.S., Tarannikov, Yu.V.: On plateaued Boolean functions with the same spectrum support. Sib. Elektron. Mat. Izv. **13**, 1346–1368 (2016)
7. Krichevsky, R.: Universal compression and retrieval. Kluwer Academic Publishers, Dordrecht (1994)
8. Langevin, P., Leander, G., Rabizzoni, P., Veron, P., Zanotti, J.-P.: Counting all bent functions in dimension eight 99270589265934370305785861242880. Des. Codes Cryptography **59**(1–3), 193–205 (2011)
9. Li, L., Huang, X., Zhao, Q., Zheng, D.: Two classes of 1-resilient semi-bent functions based on disjoint linear codes. Discret. Appl. Math. **358**, 147–157 (2024)
10. Mesnager, S.: Bent Functions: Fundamentals and Results. Springer International Publishing, Switzerland (2016)
11. Mesnager, S., Özbudak, F., Sinak, A., Cohen, G.: On q-ary plateaued functions over F_q and their explicit characterizations. European J. Combin. **80**, 71–81 (2019)
12. Potapov, V.N.: An upper bound on the number of bent functions. In: Proc. XVII International Symposium on Problems of Redundancy in Information and Control Systems. pp. 95–96. Moscow, Russia, IEEE (2021)
13. Potapov, V.N., Avgustinovich, S.V.: Combinatorial designs, difference sets, and bent functions as perfect colorings of graphs and multigraphs. Siberian Math. J. **61**(5), 867–877 (2020)
14. Potapov, V.N., Taranenko, A.A., Tarannikov, Yu.V.: Asymptotic bounds on numbers of bent functions and partitions of the Boolean hypercube into linear and affine subspaces. Des. Codes and Cryptogr. **92**(3), 639–651 (2024) Special Issue: Coding and Cryptography 2022
15. Potapov, V.N., Özbudak, F.: Asymptotic lower bounds on the number of bent functions having odd many variables over finite fields of odd characteristic. Cryptography and Communications, 2024, Boolean Functions and Their Applications VIII. (2024). https://doi.org/10.1007/s12095-024-00726-x
16. Potapov, V.N.: Existence of balanced functions that are not derivative of bent functions. In: Proc. 2023 XVIII International Symposium on Problems of Redundancy in Information and Control Systems. IEEE, Moscow, Russia (2023)
17. Tokareva, N.N.: On the number of bent functions from iterative constructions: lower bounds and hypothesis. Adv. Math. Commun. **5**(4), 609–621 (2011)
18. Tokareva, N.: Bent functions: results and applications to cryptography. Academic Press, Inc., Orlando, FL, United States (2015)

19. Tokareva, N.N.: On the set of derivatives of a Boolean bent function. Prikl. Diskretn. Mat. Suppl. **9**, 327–350 (2016) (in Russian)
20. Tsfasman, M.A., Vladuts, S.G.: Algebraic geometric codes. Basic notations. Mathematical Surveys and Monographs, vol. 139. American Mathematical Society, Providence (2007)
21. Shaporenko, A.: Derivatives of bent functions in connection with the bent sum decomposition problem. Des. Codes Cryptogr. **91**(5), 1607–1625 (2023)
22. Zhang, F., Pasalic, E., Bapic, A., Wang, B.: Constructions of several special classes of cubic bent functions outside the completed Maiorana-McFarland class. Inform. Comput. **297**, 105149 (2024)